

TC2100

Bldg. A806PH

RANDOLPH

Organization

U. S. DEPARTMENT OF COMMERCE

COMMISSIONER FOR PATENTS

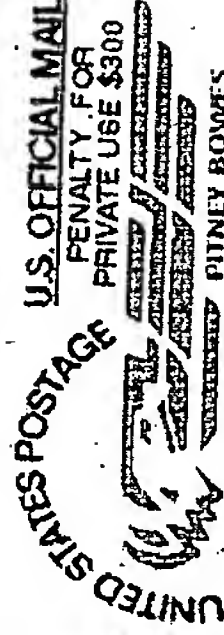
P.O. BOX 1450

ALEXANDRIA, VA 22313-1450

IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

AN EQUAL OPPORTUNITY EMPLOYER



02 1A \$ 00.87<sup>0</sup>

0004204479 JAN 29 2007

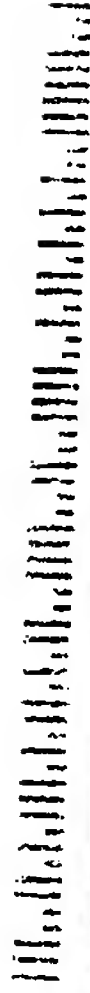
MAILED FROM ZIP CODE 22314

FEB 06 2007

NIXIE

3017 1 14 02/03/97

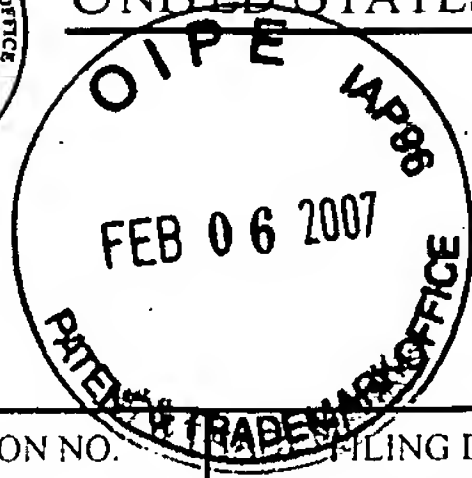
RETURN TO SENDER  
NOT DELIVERABLE AS ADDRESSED  
UNABLE TO FORWARD  
RETURN TO SENDER



FOE



# UNITED STATES PATENT AND TRADEMARK OFFICE



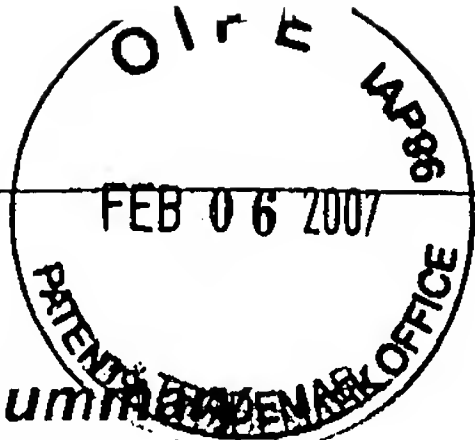
*TFJ*

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

|  |             |                      |                     |                  |
|--|-------------|----------------------|---------------------|------------------|
| APPLICATION NO.  | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
| 10/605,935   | 11/06/2003  | Leon Chernyak        |                     | 2934             |
| 34069  | 7590        | 01/29/2007           | EXAMINER            |                  |
| LEON CHERNYAK<br>112 ACADEMY HILL RD. #1<br>BRIGHTON, MA 02135 |             |                      | LANIER, BENJAMIN E  |                  |
|  |             |                      | ART UNIT            | PAPER NUMBER     |
|  |             |                      | 2132                |                  |
| SHORTENED STATUTORY PERIOD OF RESPONSE                         |             | MAIL DATE            | DELIVERY MODE       |                  |
| 3 MONTHS   |             | 01/29/2007           | PAPER               |                  |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.



# Office Action Summary

Application No.

10/605,935

Applicant(s)

CHERNYAK ET AL.

Examiner

Benjamin E. Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-43 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24, 29-31 and 39-43 is/are rejected.
- 7) ☒ Claim(s) 25-28 and 32-38 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 November 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_.

## **DETAILED ACTION**

### ***Specification***

1. The abstract of the disclosure is objected to because it exceeds 150 words in length.

Correction is required. See MPEP § 608.01(b).

### ***Oath/Declaration***

2. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:

There are no inventor signatures or a showing or indication that it was signed (37 CFR 1.63).

### ***Claim Objections***

3. Claims 25-28, 32-38 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative only. See MPEP § 608.01(n). Accordingly, the claims have not been further treated on the merits.
4. Claim 42 is objected to because of the following informalities: Claim 42 is a system claimed but is claimed as a method. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 112***

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2132

7. Claim 12 recites the limitation "said index" in line 2. There is insufficient antecedent basis for this limitation in the claim.

*Claim Rejections - 35 USC § 102*

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-24, 29-31, 39, 40-43 are rejected under 35 U.S.C. 102(b) as being anticipated by Hoffstein, U.S. Patent No. 6,298,137. Referring to claim 1, 6, 8, 10, 11-14, 16-24, 29-31, 40-42, Hoffstein discloses a ring-based public key cryptosystem where communication of information is provided between users by generating a ring  $R$ , ideals  $P$  and  $Q$  in  $R$ , a set of coset representatives  $C_q$  for the ring  $R$  modulo the ideal  $Q$ , and a set of coset representatives  $C_p$  for the ring  $R$  modulo the ideal  $P$ , generating at least one public key element  $h_1, \dots, h_k$  in the ring  $R$  as a function of at least two private key elements  $f_1, \dots, f_n$  in  $R$  and the ideal  $Q$  of the first user (Abstract), generating an element  $e$  in  $R$  as a function of the ideals  $P$  and  $Q$ , and the public key elements  $h_1, \dots, h_k$  (Abstract), a private message element  $m$  in  $R$ , and at least one private random element  $\phi_1, \dots, \phi_I$  of the second user, which meets the limitation of generating a module  $V$  over a ring  $R$ , generating an outer component  $P$  of encryption key that includes sequence  $(p_1, p_2, \dots, p_k)$  where each member  $p_j$  of the sequence belongs to the set  $\{1, 2, \dots, m\}$ , generating an inner component  $Q$  of encryption key that includes elements  $v_1, v_2, \dots, v_m$  of  $V$  and automorphisms  $g_1, g_2, \dots, g_m$  of  $V$ , generating the encryption key  $K=(P, Q)$  where  $P$  is the outer component and  $Q$  is the inner component, generating an encryption automorphism  $T$  of  $V$  based



Art Unit: 2132

on the encryption key  $K$ , where  $T$  includes a composition of certain automorphisms  $T_1, T_2, \dots, T_m$  of the module  $V$ , which composition is performed in the order prescribed by  $P$ , generating automorphisms  $T_1, T_2, \dots, T_m$  of finite orders, generation of each automorphism  $T_i$  of the order 2, generating an encrypted message element  $E$  as a function of a message element  $M$  in  $V$  and of the encryption automorphism  $T$ . Transmitting the element  $e$  from the second user to the first user, such that the first user can determine the message element  $m$  by computing a result  $A$  in  $R$  of evaluating a function  $F$  of  $E, f_1, \dots, f_n$ , computing a coset representative  $a$  of  $A$  in the set of coset representatives  $C_q$ , computing a result  $B$  of evaluating a function  $G$  of  $a, f_1, \dots, f_n$ , computing a coset representative  $a$  of  $A$  in the set of coset representative  $b$  of  $B$  in the set of coset representatives  $C_q$ , and computing a result  $c$  in the set of coset representatives  $C_p$  of evaluating a function  $H$  of  $b, f_1, \dots, f_n$  (Abstract), which meets the limitation of transmitting the encrypted message element along with the outer component  $P$  from one user to another, generating the outer component  $P$  of decryption key that includes sequence  $(pk, pk-1, \dots, p_1)$ , generating the decryption key  $K'=(P';Q')$ , where  $P'$  is the outer component of the decryption key and  $Q'$  is the inner component of the decryption key which is equal to the inner component  $Q$  of the encryption key, generating a decryption automorphism  $T_d$  of  $V$  based on the decryption key  $K'$ , where  $T_d$  includes a composition of automorphism  $T_1, T_2, \dots, T_m$ , which composition is performed in the order prescribed by  $P'$ , determining the message element  $M$  as a function of the encrypted message element  $E$  and of the decryption automorphism  $T_d$ , where the function is the same as that one used in generation of  $E$ .

Art Unit: 2132

Referring to claim 2, Hoffstein discloses that the ring is a ring of polynomials with integer coefficient modulo the ideal consisting of all multiples of  $(x^n) - 1$  (Col. 5, lines 46-49), which meets the limitation of the ring R is any commutative or non-commutative ring.

Referring to claim 3, Hoffstein discloses that an element in ring R is a vector (Col. 4, lines 56-59), which meets the limitation of V is a projective module over the ring R.

Referring to claim 4, Hoffstein discloses that dimension of the system is greater than 1 (Col. 10, lines 35-39), which meets the limitation of V is a free R-module of dimension n, and where n is an integer greater than 1.

Referring to claim 5, Hoffstein discloses that the vector is an element comprising a set of elements in the ring R (Col. 4, lines 55-64), which meets the limitation of the R-module V is the standard free module R, where V is the set of all n-tuples  $x=[x_1, x_2, \dots, x_n]$  of elements of R.

Referring to claim 7, Hoffstein discloses that elements f and g of the ring are generated and generating element  $F_q$ , which is an inverse of f (mod q), and generating  $F_p$ , which is an inverse of f (mod p) (Col. 3, lines 2-5), which meets the limitation of said ring R is the skew field of quaternions.

Referring to claim 9, Hoffstein discloses that the ring is a ring of matrices (Col. 8, lines 64-65), which meets the limitation of the ring R is the ring of matrices over the field of real numbers.

Referring to claims 15, 39, 43, Hoffstein discloses that the encrypted message is transmitted from one user to another over a channel (Figure 1 & Col. 11, lines 15-16).

### ***Conclusion***

Art Unit: 2132

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Paar, U.S. Patent No. 7,069,287

Koh, U.S. Patent No. 7,136,484

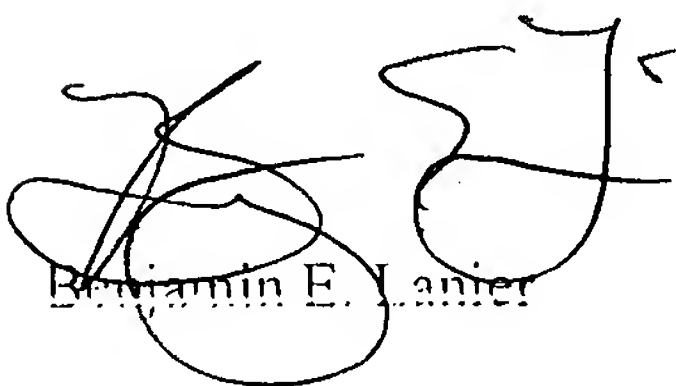
Paeng, U.S. Publication No. 2004/0156498

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

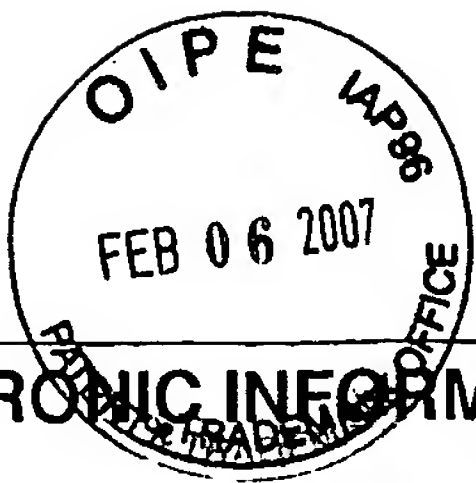
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier





IDS - 11/06/2003

**ELECTRONIC INFORMATION DISCLOSURE STATEMENT**

Electronic Version v18  
Stylesheet Version v18.0

| <b>Title of<br/>Invention</b>  | Geometry-Based Symmetric Cryptosystem Method |            |            |                  |      |          |          |       |          |    |   |         |            |     |  |  |  |  |   |         |            |                  |  |  |  |   |   |         |            |                 |  |  |  |               |      |                   |            |
|--|--|------------|------------|------------------|------|----------|----------|-------|----------|----|---|---------|------------|-----|--|--|--|--|---|---------|------------|------------------|--|--|--|---|---|---------|------------|-----------------|--|--|--|---------------|------|-------------------|------------|
| <p>Application Number :<br/>Confirmation Number:<br/>First Named Applicant:            Leon Chernyak<br/>Attorney Docket Number:<br/>Art Unit:<br/>Examiner:<br/>Search string:                    ( 5740250 or 6038317 or 6298137 ).pn</p> <p><b>US Patent Documents</b></p> <p>Note: Applicant is not required to submit a paper copy of cited US Patent Documents</p> <table border="1"><thead><tr><th>init</th><th>Cite.No.</th><th>Patent No.</th><th>Date</th><th>Patentee</th><th>Kind</th><th>Class</th><th>Subclass</th></tr></thead><tbody><tr><td>BL</td><td>1</td><td>5740250</td><td>1998-04-01</td><td>Moh</td><td></td><td></td><td></td></tr><tr><td></td><td>2</td><td>6038317</td><td>2000-03-01</td><td>Magliveras et al</td><td></td><td></td><td></td></tr><tr><td>✓</td><td>3</td><td>6298137</td><td>2001-10-01</td><td>Hoffstein et al</td><td></td><td></td><td></td></tr></tbody></table> <p><b>Signature</b></p> <table border="1"><thead><tr><th>Examiner Name</th><th>Date</th></tr></thead><tbody><tr><td>/Benjamin Lanier/</td><td>01/17/2007</td></tr></tbody></table> |  | init       | Cite.No.   | Patent No.       | Date | Patentee | Kind     | Class | Subclass | BL | 1 | 5740250 | 1998-04-01 | Moh |  |  |  |  | 2 | 6038317 | 2000-03-01 | Magliveras et al |  |  |  | ✓ | 3 | 6298137 | 2001-10-01 | Hoffstein et al |  |  |  | Examiner Name | Date | /Benjamin Lanier/ | 01/17/2007 |
| init   | Cite.No.                                     | Patent No. | Date       | Patentee         | Kind | Class    | Subclass |       |          |    |   |         |            |     |  |  |  |  |   |         |            |                  |  |  |  |   |   |         |            |                 |  |  |  |               |      |                   |            |
| BL   | 1  | 5740250    | 1998-04-01 | Moh              |      |          |          |       |          |    |   |         |            |     |  |  |  |  |   |         |            |                  |  |  |  |   |   |         |            |                 |  |  |  |               |      |                   |            |
|  | 2  | 6038317    | 2000-03-01 | Magliveras et al |      |          |          |       |          |    |   |         |            |     |  |  |  |  |   |         |            |                  |  |  |  |   |   |         |            |                 |  |  |  |               |      |                   |            |
| ✓  | 3  | 6298137    | 2001-10-01 | Hoffstein et al  |      |          |          |       |          |    |   |         |            |     |  |  |  |  |   |         |            |                  |  |  |  |   |   |         |            |                 |  |  |  |               |      |                   |            |
| Examiner Name  | Date   |            |            |                  |      |          |          |       |          |    |   |         |            |     |  |  |  |  |   |         |            |                  |  |  |  |   |   |         |            |                 |  |  |  |               |      |                   |            |
| /Benjamin Lanier/  | 01/17/2007                                   |            |            |                  |      |          |          |       |          |    |   |         |            |     |  |  |  |  |   |         |            |                  |  |  |  |   |   |         |            |                 |  |  |  |               |      |                   |            |

# **Notice of References Cited**

Application/Control No.

10/605,935

Applicant(s)/Patent Under

Reexamination

CHERNYAK ET AL.

Examiner

Benjamin E. Lanier

FEB 06 2007

Art Unit

2132

Page 1 of 1

## **U.S. PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name             | Classification |
|---|---|--|-----------------|------------------|----------------|
| * | A | US-6,298,137                                     | 10-2001         | Hoffstein et al. | 380/30         |
| * | B | US-7,069,287                                     | 06-2006         | Paar et al.      | 708/492        |
| * | C | US-7,136,484                                     | 11-2006         | Koh, Jee H.      | 380/28         |
| * | D | US-2004/0156498                                  | 08-2004         | Paeng et al.     | 380/030        |
|   | E | US-  |                 |                  |                |
|   | F | US-  |                 |                  |                |
|   | G | US-  |                 |                  |                |
|   | H | US-  |                 |                  |                |
|   | I | US-  |                 |                  |                |
|   | J | US-  |                 |                  |                |
|   | K | US-  |                 |                  |                |
|   | L | US-  |                 |                  |                |
|   | M | US-  |                 |                  |                |

## **FOREIGN PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--|-----------------|---------|------|----------------|
|   | N |  |                 |         |      |                |
|   | O |  |                 |         |      |                |
|   | P |  |                 |         |      |                |
|   | Q |  |                 |         |      |                |
|   | R |  |                 |         |      |                |
|   | S |  |                 |         |      |                |
|   | T |  |                 |         |      |                |

## **NON-PATENT DOCUMENTS**

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|---|
|   | U |   |
|   | V |   |
|   | W |   |
|   | X |   |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.